



25

October 14, 2003

Office of Thrift Supervision
Chief Counsel's Office
1700 G Street, NW
Washington, D.C. 20552

Attention: No. 03-35

The Consumer Data Industry Association provides the following comments on the proposed "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice."

The CDIA is concerned that these guidelines, while issued for the important purpose of further clarifying how and when a response program should include the decision to issue a notice of a breach of personal information, will in fact operate as a limitation on the full flexibility a financial institution needs to make the right decision relative to a particular circumstance both in terms of when to issue a notice and what the content of that notice should be. Thus, the guidelines may have the unintended consequence of driving up the number of notices sent due more so to concerns about meeting the minimum standards found within the guidance and less so because of the true seriousness of the risks to a financial institution's customers. A financial institution's customers may ultimately consider frequent notices less worthy of serious consideration. While we applaud the proposed standard for providing notices, which states that "an institution should notify affected customers whenever it becomes aware of unauthorized access to sensitive customer information unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers..." we believe the examples of when notices should be given will trigger many notices even where the risks are low. It may not be particularly helpful to offer examples of when notices are or are not expected, since these can lend themselves to interpretive questions, rather than interpretive clarity.

Our members are very concerned about the effects of frequent notices and the downstream effect of high contact volumes on our members' ability to meet the requirements of law imposed on them under the Fair Credit Reporting Act¹ and to serve all consumers, millions of whom already contact nationwide consumer reporting agencies each year to request file disclosures, the

¹ 15 U.S.C. Sec. 1681 *et seq.*

placement of fraud alerts and to dispute information in their files.² It is particularly troubling that the guidance relative to “key elements” of the content of the customer notice suggests that in all cases where a notice is issued, that it should include contact information for nationwide consumer reporting agencies. Unless the trigger for determination that a notice is sufficiently robust, these notices and the ensuing contacts with our members’ national consumer assistance centers will have a deleterious effect on service levels for all consumers who, for example, are already confirmed victims of fraud or otherwise are responding to adverse action notices. We do not believe that all notices should necessarily include contact information for nationwide consumer reporting agencies.

Illustrative of our concern is a security breach incident, which involved a single company, Triwest, located in Phoenix, Arizona. Triwest had the identifying information of approximately 500,000 military families stolen. As part of their notice to customers, Triwest advised them to contact nationwide consumer reporting agencies. These notices resulted in high volumes of contacts and a cost to our members of approximately \$1.5 million per company. Our members did not cause the breach to occur and yet they bore the brunt of the costs of the breach due to their servicing of approximately 365,000 contacts. Nationwide consumer reporting agencies have always stood ready to serve consumers, but the enormous burdens associated with security breach notices, over which they have no control and no means of recouping costs, has become a serious issue that must be addressed.

Our members believe that there are key elements to establishing the appropriate balance where a financial institution has determined that a notice should be sent to its customers. These elements include:

- Coordination – breach notices that do reference contacting nationwide consumer reporting agencies should not be issued until the financial institution has contacted each nationwide consumer reporting agency to coordinate the timing, content, and staging of notices as well as the placement of fraud alerts, where necessary.
- Costs – financial institutions that believe that a notice should include contact information for nationwide consumer reporting agencies should work with them in advance to purchase the services it believes are necessary to protect its customers from the downstream effects of the breach of customer information, including the costs of file disclosures, placement of fraud alerts and other services. The costs of servicing literally millions consumers who receive notices cannot be borne by the nationwide consumer reporting agencies.³

² The CDIA estimates that nationwide consumer reporting agencies issue approximately 16 million file disclosures per year. Approximately 11 percent are issued due to concerns about fraud.

³ The costs of servicing consumers who are victims of security breaches can be as high as \$10 per consumer.

Ultimately, careful consideration of what should truly trigger a notice, coupled with coordination of communications and mitigation of costs are all key elements necessary to ensure that a national program of notices is most likely to be effective. We appreciate this opportunity to provide comment on the proposed guidance.

Sincerely,

Stuart K. Pratt
President & CEO